# Berufsziel Security Tester

Hollywood suggeriert, dass Hacker die Krönung der Informatiker-Evolution seien, denen es spielerisch gelingt, komplexe Systeme auszutricksen. Die Realität sieht anders aus.

Von Christoph Baumgartner

Eine wichtige Anmerkung vorweg: Damit technische Sicherheitsüberprüfungen nicht gesetzeswidrig sind, muss vor der Durchführung das explizite Einverständnis von Systembesitzer und -eigentümer vorliegen. Wer sich nicht daran hält, kann mit Busse oder Gefängnis bestraft werden.

## Anforderungsprofil

Ein guter Security Tester (auch Ethical Hacker, Security Analyst, Penetration Tester, Auditor etc. genannt) muss in der Lage sein, Software- und Design-basierte Schwachstellen zu erkennen sowie situativ spezifische Tools und Exploits einzusetzen und zu entwickeln. Somit werden fundierte Tool-, Programmier- und Software-Architekturkenntnisse und ein gutes Mass an Erfahrung vorausgesetzt. Da der Grossteil der technischen Audits (auch) via Netzwerk erfolgt, sind ausgeprägte Netzwerkprotokollkenntnisse essentiell. Ausserdem muss ein Tester strukturiert arbeiten und in der Lage sein, Sachverhalte präzise zu beschreiben, mit allfälligen Projektteammitgliedern zu kooperieren und mit dem Auftraggeber zu kommunizieren. Da Security Tester potentiell sozusagen Operationen am offenen Herzen der IT durchführen, müssen professionelle Security Tester selbstredend zwingend über einen tadellosen Leumund verfügen.

Technische Tools werden von Security Testern immer dann eingesetzt, wenn Automatismen den Projektfortschritt beschleunigen, ohne dass die Qualität darunter leidet. Denn kein Kunde wäre bereit, ein Vielfaches an Projektaufwand zu berappen, nur weil beispielsweise Tasks wie Port Scans manuell durchgeführt würden.

Erst danach wird es spannend, weil die Tester je nach vorgegebenen Rahmenbedingungen für das Auffinden und Verifizieren von Sicherheitslücken alle Register ihres Könnens ziehen müssen.

### IN KÜRZE

- Verschiedene Organisationen und Unternehmen bilden Security Tester aus.
- Die Anforderungen für die Ausbildung sind nicht zu unterschätzen.
- Zertifizierungen erhöhen den Marktwert eines Security Testers, machen aber Weiterbildung und Praxis nicht obsolet.

## Ausbildungsmöglichkeiten

Verschiedene Organisationen und Unternehmen bieten Kurse und Zertifizierungen an, welche den Zertifizierten als kompetenten Security Tester ausweisen sollen, der sich durch fachliches Können, ethisches Verhalten und die Einhaltung der gesetzlichen Rahmenbedingungen auszeichnet. Doch was bezwecken und bringen diese Zertifizierungen?

Stellvertretend für alle Zertifizierungsprogramme stehen in diesem Artikel zwei in der Schweiz bekannte Zertifizierungsmodelle, welche von EC-Council (http://www.eccouncil.org) und von ISECOM (http://www.isecom.org) respektive deren akkreditierten Schulungspartnern angeboten werden. EC-Council bietet für den Werdegang des Security Testers ein hierarchisch aufgebautes Zertifizierungsprogramm an. ISECOM setzt auf verschiedene, einander gleichgestellte Spezialisierungsrichtungen.

## EC-Council

Das «International Council of E-Commerce Consultants» (EC-Council) hat ihre Hauptsitze in Albuquerque (USA), Hyderabad (Indien) und Selangor (Malaysia). Die erste Ausbildungsstufe zum professionellen Security Tester bildet der Zertifizierungskurs «Certified Ethical Hacker» (CEH). Anschliessend kann die Zertifizierung zum «EC-Council Certified Security Analyst» (ECSA) erlangt werden. Wer beide Zertifizierungen besitzt, kann sich als «Licensed Penetration Tester» (LPT) zertifizieren lassen.

## ISECOM

Das «Institute for Security and Open Methodologies» (ISECOM) ist eine Non-Profit-Organisation mit Hauptsitz in Barcelona (Spanien) und Zweigstelle in New York (USA). Das «Open Source Security Testing Methodology Manual» (OSSTMM) ist eine von Fachleuten laufend überprüfte und erweiterte, weltweit anerkannte Methode zur Planung und Durchführung von Sicherheits-überprüfungen sowie der Bewertung und Dokumentation der Ergebnisse. Der frei verfügbare De-facto-Standard OSSTMM existiert seit Ende 2000 und wird unter der Leitung von ISECOM kontinuierlich weiterentwickelt. Das OSSTMM gehört zum Lehrplan und Prüfungsstoff von fast allen seitens ISECOM angebotenen personenbezogenen Zertifizierungen. Folgende OSSTMM-bezogenen Zertifizierungen für professionelle Security Tester werden angeboten: «OSSTMM Professional Security Tester» (OPST), «OSSTMM Professional Security Analyst» (OPSA) und «OSSTMM Wireless Security Expert» (OWSE). Die Zertifizierung zum «OSSTMM Professional Security Expert» (OPSE) ist primär für Leute wie etwa Projektleiter gedacht, welche sich hinsichtlich der richtigen theoretischen Anwendung der im OSSTMM definierten Methode zertifizieren lassen möchten, ohne selbst aktiv an den Tests teilzunehmen.

## Voraussetzungen

Die Kurse OPST, OPSA, OWSE, CEH und ECSA setzen technische Kenntnisse voraus, weil sie für (angehende) Security Tester gedacht sind. Zumindest sollten die Kursteilnehmer die Betriebssysteme Windows und/oder Linux als Power-User aufsetzen und nutzen können und

**Ethical Hacker überprüfen die getroffenen Massnahmen für die IT-Sicherheit.**

sich rudimentär mit Netzwerkprotokollen auskennen. Andernfalls lässt sich der dichtgepackte Lehrstoff nicht begreifen und durcharbeiten. Bei allen Kursen wird die Anwendung diverser Tools und/oder die Analyse und Interpretation diverser Tool-Outputs erlernt und gefordert. Die Grösse des Werkzeugkastens eines Security Testers umfasst Dutzende bis Hunderte von Tools, wobei realistischerweise während der Kurse höchstens zwei Dutzend Werkzeuge aktiv eingesetzt werden.

## Zielgruppen

Die Zertifizierungen CEH, OPST und OWSE sind für Security Tester gedacht, welche selbst Tests des Qualitätslevels Penetration Test, Ethical Hacking oder Application Security Audit durchführen, weil dabei viel Kurszeit auf die Vorstellung der für die einzelnen Testphasen Information Gathering, Enumeration, Vulnerability Detection & Verification benötig-ten Techniken und Tools verwendet wird. Die Kursinhalte OPSA und ECSA legen den Schwerpunkt hingegen auf die Analyse von Testergebnissen und Tool-Outputs sowie deren korrekte Interpretation. Neben technischen werden dabei auch kommerzielle Aspekte beleuchtet.

## Aufwand und Kosten

Die Zertifizierungskurse zum CEH, ECSA, OPST oder OPSA dauern alle ca. 5 Tage und kosten je nach Anbieter in der Schweiz inkl. Prüfungsgebühr zwischen 5000 und 7000 Franken. Der zusätzlich zu veranschlagende Lern- und Übungsaufwand seitens der Teilnehmer ist individuell und direkt abhängig vom Wissens- und Übungsstand. Es sollten aber im Minimum 2 bis 4 Stunden Zusatzaufwand pro Tag veranschlagt werden, um reelle Chancen zu wahren, die Zertifizierungsprüfung zu bestehen.

## Nutzen

Insbesondere Neulingen im Security-Tester-Gebiet bieten diese Zertifizierungskurse eine gute Gelegenheit, innert kurzer Zeit eine beachtliche Auswahl an sogenannten «Hacker Tools» kennenzulernen und zu erfahren, wie Security-Test-Projekte methodisch korrekt geplant, durchgeführt und auch – besonders wichtig – dokumentiert werden.

In der Akquisitionsphase für zukünftige Security Audits sind derartige Zertifizierungen aus Sicht der potentiellen Auftraggeber bei stimmigem Angebot sicherlich ein Grund mehr, sich für die besagte Firma zu entscheiden. Dies gilt insbesondere für Security-Test-Anbieter, welche noch nicht mit beeindruckenden Referenzen punkten können. Die ISECOM wird regelmässig von potentiellen Arbeitgebern angefragt, welche auf der Suche nach OPSx-Zertifizierten sind – ISECOM agiert in derartigen Fällen als kostenloser Vermittler zwischen Arbeitgeber und Job-Interessierten –, wobei selbstverständlich die Diskretion gewahrt wird. EC-Council publiziert Stellenangebote auf ihrer Website. Falls die OPSx-Zertifizierten dies explizit wünschen, werden sie kostenlos auf der Website von ISECOM zu Verifikationszwecken mit Namen, Zertifizierung und Zertifizierungsdatum genannt.

## Fazit

Die in diesem Artikel genannten Zertifizierungen sind ein Leistungsausweis und kein Gefälligkeitszeugnis. Dennoch ist die bestandene Zertifizierungsprüfung provokativ ausgedrückt nur ein bedingter Fähigkeitsausweis, weil die Zertifizierung lediglich besagt, dass der Zertifizierte die Prüfungsaufgaben erfolgreich gemeistert hat, nicht aber, ob die Person im Alltag unter beliebigen Rahmenbedingungen korrekt, gewissenhaft und effizient Security Tests durchführen und dokumentieren kann. Diese Fähigkeiten lassen sich nur durch ständige Übung und Erfahrung entwickeln und perfektionieren. Es sollte sich also niemand der Illusion hingeben, dass die bestandene Prüfung jemanden automatisch zum «Meisterhacker» macht – auch wenn insbesondere die von EC-Council angebotenen Zertifizierungen dies suggerieren. Alle genannten Zertifizierungskurse bieten aber eine solide Grundlage, auf der angehende Security Tester aufbauen können.

Christoph Baumgartner ist Mitglied des ISECOM Core Teams und CEO der auf technische Audits spezialisierten OneConsult GmbH, www.oneconsult.com.